SECURE COALITION ID
Protecting Identity with Technology

Comments of the Secure ID Coalition to the California Research Bureau Advisory Board established to evaluate Security and Privacy Recommendations for Government-Issued Radio Frequency Identification (RFID)-Enabled Documents

The California Research Bureau (CRB) has been tasked with an important directive to prepare and deliver a report on security and privacy recommendations for government-issued, radio frequency identification (RFID)-enabled identity documents (IDs). The Advisory Board, as outlined in the letter from Senator Joseph Simitian, has an enormous responsibility that could potentially impact every citizen of the State of California.

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents. **Our mission is to promote the understanding and appropriate use of identity technology that achieves enhanced security for ID management systems while maintaining user privacy.** Members of our coalition manufacture many different varieties of ID technologies and are thus are uniquely positioned to offer expertise in this area.

The problem posed to the CRB Advisory Board raises important questions about the technologies available to be used for human identification. It is important to note that there are currently many international standards that govern identification documents in the US, and around the world. These standards were established after significant technical review processes. Likewise, there are many programs within the U.S. Government that have undergone extensive evaluations of identification document technologies. The most substantial of which include the Department of Defense's Common Access Card (CAC), the Department of State's electronic Passport and the Department of Homeland Security's Transportation Worker Identification (TWIC). Further, the entire federal government went through an extensive evaluation program as part of developing the standards for their own employee identification credential under Homeland Security Presidential Directive -12 (HSPD-12) and resulting in Federal Identification Processing Standard 201 (FIPS 201).

Whenever there has been a serious evaluation of identification technologies for government programs anywhere in the world, smart cards have been chosen as the solution because of the technology's unique ability to securely protect information and their ability to provide only the information that the reader integrating the document is allowed to receive. This prevents unauthorized readers from gaining access to any information on the chip inside the card.

Exactly what is a smart card? Simply put, smart card technology consists of a sophisticated electronic computer chip embedded in a plastic card body. The chip has an operating system which provides the features and functions for a particular application, such as entering a building, logging onto a computer network, conducting e-government enabled business transactions or crossing a border. The success of smart card technology is its ability to provide strong security and privacy protections to each individual, in a convenient card-form. You may consider the computer chip as an electronic security agent, representing the issuer of the ID, in the hands of the user. The chip security and communication protocols ensure information security and privacy. Some cards communicate either directly (contact) to a reading device or over short range wireless connections (contactless).

In this case, the CRB Advisory Board has been asked to examine the contactless version of smart cards that uses radio frequency in the high frequency (HF) range as it is the closest to RFID. Whatever method used in a secure smart card, the underlying security ensures both electronic document authentication and user authentication before transacting any credential information. No other technology can offer all these features in a cost effective and convenient manner to ensure identity security and authentication.

Smart card design is based on national and international standards allowing for an open and competitive supply of the chips, cards, operating systems and security features. Common standards and specifications that smart card systems adhere to include the following:

- International Standards Organization (ISO) 7810 – specifies the card form factor
- ISO 7816 – Smart card multi part standard – physical, electrical, protocol and cryptography
- ISO 14443 – Contactless smart card interface – physical, electrical and protocol
- Java Card V2.X specification
- Global Platform specification
- FIPS 140-2 – Cryptographic integrity
- FIPS 201 – PIV II (Card standard for Federal Government)
- International Civil Aviation Organisation (ICAO) 9303 – Machine readable travel documents

Specific implementations may then extend this list with custom application specifications made for particular applications.

In some cases however, there have been movements away from identity document standards towards other technology solutions that were designed to address other problems not the identification of people. Most notable of these types of technologies is the ultra-high frequency (UHF) -RFID, which was designed for supply-chain management, the tracking of products and pallets in a warehouse. UHF-RFID was never intended to identify people; as such the technology was designed to be read at long distance with little or no security. UHF-RFID tags use a simple consistent number that is transmitted every time it is stimulated by a power source to track that which it is attached or associated. The number transmitted is the same number every time and designed to be read easily so the technology does not incorporate security features or privacy protections designed to protect the number. While this technology is excellent for tracking products and pallets, it is an inappropriate technology for identifying people.

People require more security than dog food. Citizen privacy rights must be the first and foremost consideration when designing, evaluating and implement identity systems. It is the position of the Secure ID Coalition that any identity management system used for the identification of a person must incorporate the highest level of security features and protections for personal privacy.

Because UHF-RFID chip technology was designed to be used in little-to-no security applications, safety measures were not built into the chip architecture. When used in any security application, it becomes vulnerable to skimming, cloning, spoofing, and denial of service attacks that enable criminals, terrorists and thugs to exploit these vulnerabilities, thus rendering protected assets less secure, not more. For example, a common tactic by those trying to mitigate the security vulnerabilities of UHF- RFID solutions is to use a unique identifier for each user. The unique identifier is the same number every time the card is presented, and much like the Social Security number, that number is associated with the individual. Unfortunately, because the security on a UHF-RFID chip is almost non-existent, the unique identifier can be easily read by any off-the-shelf reader purchased over the Internet. Once the number is ascertained, creating a new card or document with the skimmed unique number can be done in a matter of minutes. The protected asset is now open to vulnerabilities from these fraudulent ID documents.

In contrast, because smart cards were designed to identify people, the cards not only incorporate dozens of physical security features but also electronic security features that can further protect the document and the user. The information on the chip can also be encrypted so that it can not be skimmed, hacked or altered. Critically, the information on the card cannot be skimmed during transmission as smart cards require mutual authentication (a "hand-shake" exchange between the card and the reader attempting to access the card), to confirm that both are legitimate and have not be tampered with or altered. Further, any information that is transmitted over the air-waves in an RF-enabled capacity is protected with an encrypted channel so that the information is not sent in the clear.

Smart cards protect card-holders' privacy by "firewalling" information, only providing access to the necessary information for the transaction approved by the card-holder. External parties requesting information from the smart card must be authenticated prior to any information being exchanged. Then, in accordance with the transaction for which the reader is authorized, ONLY information pertaining to that specific transaction is communicated. No other information can be accessed. Finally, the information on the card can further be protected by a PIN code or a biometric that convinces the card of that the *authorized* user is present before any transaction can take place.

It is for these reasons that the Secure ID Coalition encourages the CRB Advisory Board to closely review the need for security and privacy in identification documents. **While public policy initiatives and regulations should reflect a technology-neutral stance, it is critical that the CRB Advisory Board understand that only smart card identification technology solutions are successfully being used around the world today, as only they can enable both enhanced privacy protections and security in an RF-enabled format.** Attached for your review are the formal documents filed by the Secure ID Coalition as part of the Department of State's Notice of Proposed Rulemaking (NPRM) proceedings on the Western Hemisphere Travel Initiative and the Department of Homeland Security's NPRM on REAL ID.

We are pleased to offer the expertise of the Secure ID Coalition to the CRB Advisory Board and look forward to working with you as you begin to evaluate the nexus between the need for identification documents, security and privacy. If there any questions related to the information in this overview or the attached documents please do not hesitate to contact the Secure ID Coalition's Executive Director Kelli Emerick at 202-262-9115.